(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－295202
（P2000－295202A）
(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｋ　1/04		Ｈ０４Ｋ　1/04		５Ｃ０５９
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	５Ｃ０６４
// Ｈ０４Ｎ　7/24		7/13	Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－95756

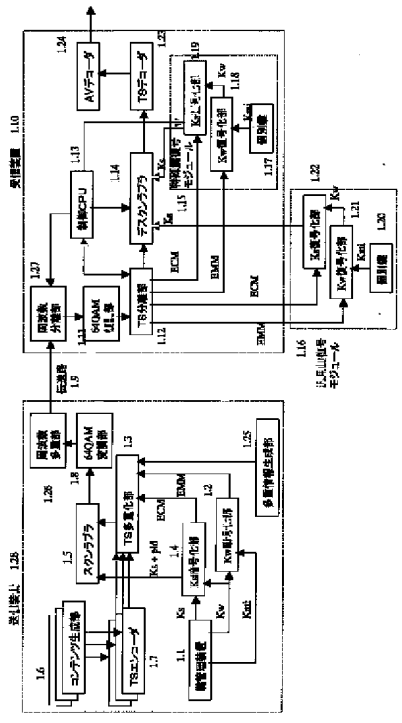
(22)出願日　平成11年４月２日(1999.4.2)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　櫻井　厚典
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

Ｆターム(参考)　5C059 KK43 MA00 RB02 RB10 RC35 RD03 RF21 SS02 SS24 UA05 UA38
5C064 CA14 CB01 CB08 CC02 CC04
5J104 AA01 BA03 EA16 NA02 NA35 NA37 PA05 PA06

(54)【発明の名称】　限定受信システム

(57)【要約】
【課題】　複数のスクランブルされたチャンネルの選択を切り替える時に選択したチャンネルのストリームを短時間でデスクランブルする限定受信システムを提供する。
【解決手段】　送信装置は各チャンネル共通のスクランブル鍵を用いて共通情報を送信し、受信装置は、汎用鍵復号モジュール116と特殊鍵復号モジュール115との２種類の復号手段を持つ。特殊鍵復号モジュールは現在受信中のチャンネルを直接検知する手段113を持ち、また、チャンネルを変更しても前回受信したスクランブル鍵を保持する。受信装置では、特殊鍵復号モジュールを用いて復号する場合、チャンネルを変更しても、そのチャンネルの視聴権がある場合には新たな共通情報の受信を待たずに、チャンネル変更前から保持されたスクランブル鍵を用いてコンテンツストリームをデスクランブルする。



【特許請求の範囲】
【請求項１】　複数のチャンネルデータをスクランブルするための鍵データを生成する鍵生成手段と、前記鍵データを用いてチャンネルデータをスクランブルするスクランブル手段とを具備する送信装置と、複数のチャンネルの中から選択した任意のチャンネルを前記鍵データを用いてデスクランブルするデスクランブル手段を具備する受信装置とから成る限定受信システムにおいて、
送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置が、前記共通の鍵データを保持する鍵保持手段を備え、いずれのチャンネルを選局した場合でも前記鍵保持手段に保持された共通の鍵データを用いてデスクンランブルすることを特徴とする限定受信システム。
【請求項２】　前記送信装置は、鍵データを格納する関連情報の中に前記共通の鍵データを含めて送信し、前記受信装置は、前記関連情報から取得した前記共通の鍵データを前記鍵保持手段で保持することを特徴とする請求項１に記載の限定受信システム。
【請求項３】　前記送信装置は、鍵データを格納した関連情報に前記鍵データが共通の鍵データであるか否かを示す識別情報を含めて送信し、前記受信装置は、共通の鍵データを示す識別情報が含まれた関連情報から前記鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに前記関連情報から鍵データを取得する汎用鍵復号モジュールとを具備し、前記関連情報に共通の鍵データを示す識別情報が含まれているときは、前記特殊鍵復号モジュールによって取得され、前記鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、前記関連情報に共通の鍵データを示す識別情報が含まれていないときは、前記汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルすることを特徴とする請求項２に記載の限定受信システム。
【請求項４】　前記送信装置は、鍵データを格納した関連情報を送信し、前記受信装置は、前記関連情報から前記鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに前記関連情報から鍵データを取得する、実装可能な汎用鍵復号モジュールと、前記汎用鍵復号モジュールの実装の有無を検出する検出手段とを具備し、前記検出手段が、前記汎用鍵復号モジュールの実装を検出していないときは、前記特殊鍵復号モジュールによって取得され、前記鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、前記検出手段が、前記汎用鍵復号モジュールの実装を検出しているときは、前記汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルすることを特徴とする請求項２に記載の限定受信システム。
【請求項５】　前記受信装置の受信チャンネルが変更された場合に、前記特殊鍵復号モジュールは、現在受信中のチャンネルに関する情報を受けて、視聴の可否を判断することを特徴とする請求項３または４に記載の限定受信システム。
【請求項６】　前記受信装置は、受信チャンネルの変更後に受信した前記関連情報に基づいて、視聴の可否を確認し、視聴権が無ければデスクランブルを停止することを特徴とする請求項５に記載の限定受信システム。
【請求項７】　前記送信装置は、前記関連情報に番組識別情報を含めて送信し、前記特殊鍵復号モジュールを持たずに、前記汎用鍵復号モジュールのみを具備する受信装置は、前記番組識別情報から視聴の可否を判断することを特徴とする請求項３または４に記載の限定受信システム。
【請求項８】　前記汎用鍵復号モジュールが、ＩＣカードで構成され、前記受信装置は、前記ＩＣカードを挿入するスロットを具備することを特徴とする請求項３、４または７に記載の限定受信システム。
【請求項９】　前記受信装置は、プログラムダウンロード手段を備え、前記送信装置からのダウンロードにより前記特殊鍵復号モジュールを置き換えることを特徴とする請求項３、４、５または７に記載の限定受信システム。
【請求項１０】　前記特殊鍵復号モジュールと受信装置のデスクランブラとがＰＣＭＣＩＡカードに実装され、前記受信装置は、前記ＰＣＭＣＩＡカードのスロットを具備することを特徴とする請求項３または４に記載の限定受信システム。
【請求項１１】　前記送信装置は、前記共通の鍵データを格納した関連情報にバージョン情報を含めて送信し、前記受信装置は、前記バージョン番号が更新されるまで、前記鍵保持手段で保持された同一の共通の鍵データを用いてデスクランブルを続けることを特徴とする請求項２に記載の限定受信システム。
【請求項１２】　前記送信装置は、前記共通の鍵データを格納した関連情報に複数種類のスクランブル鍵を含めて送信し、前記受信装置は、前記複数種類のスクランブル鍵を前記鍵保持手段で保持し、コンテンツデータパケットの非スクランブル部の情報からどのスクランブル鍵が用いられているかを識別して、デスクランブルに用いるスクランブル鍵を選択することを特徴とする請求項２に記載の限定受信システム。
【請求項１３】　前記受信装置は、番組多重情報を保持する番組多重情報保持手段を備え、番組多重情報が更新された時以外は、前記番組多重情報保持手段に保持された番組多重情報を基に選局することを特徴とする請求項２に記載の限定受信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ケーブルテレビ、

衛星放送、地上放送等において、番組をスクランブルして放送し、視聴権を持つ場合にのみデスクランブルを可能にする限定受信システムに関し、特に、チャンネルを切り替えたときに、迅速にデスクランブルが開始できるようにしたものである。

【０００２】

【従来の技術】従来の標準的な限定受信方法であるＭＰＥＧ２ＳＹＳＴＥＭＳ（ISO/IEC13818-1）では、送出側は、映像、データ等のコンテンツをスクランブル鍵Ｋｓでスクランブルして送信し、また、このスクランブル鍵ＫｓをＥＣＭ（Entitlement Control Messages：共通情報）に格納した後、この共通情報ＥＣＭをワーク鍵Ｋｗで暗号化して送信する。また、このワーク鍵Ｋｗは、事前に、ＥＭＭ（Entitlement Management Messages：個別情報）に格納した後、Ｋｍｉで暗号化して送信される。

【０００３】一方、受信側では、暗号化された個別情報ＥＭＭを受信すると、あらかじめ持っている個別鍵Ｋｍｉで復号化し、ＥＭＭからワーク鍵Ｋｗを取り出して保持する。また、暗号化された共通情報ＥＣＭと、スクランブルされたコンテンツストリームとを受信すると、ＥＣＭをワーク鍵Ｋｗで復号化してＥＣＭからスクランブル鍵Ｋｓを取り出し、スクランブルされているコンテンツストリームを、取り出したＫｓを用いてデスクランブルする。デスクランブルされた映像は、ＡＶデコーダによって視聴可能なアナログ信号に変換される。

【０００４】

【発明が解決しようとする課題】従来の標準的な限定受信方式では、チャンネルを切り替えた場合に、その都度、新たにＥＣＭからスクランブラ鍵Ｋｓを取得しているため、デスクランブルが再開されるまでに時間が掛かるという問題があった。

【０００５】また、この問題を避けるために、送信側でＥＣＭを用いる標準的な方法では無く、チャンネル視聴可否を直接制御する独自の方式を採ると、受信側では、送信側の方式に合わせた独自方式の受信装置でしか対応することができなくなり、ＥＣＭを用いる標準的な限定受信方式の受信装置では限定受信ができなくなるという問題が生じる。

【０００６】本発明は、こうした問題点を解決するものであり、チャンネルを切り替えた場合のデスクランブルを迅速に行うことができ、また、ＥＣＭを用いる標準的な限定受信方式の受信装置でも限定受信処理自体は支障なく行うことができる限定受信システムを提供することを目的としている。

【０００７】

【課題を解決するための手段】そこで、本発明の限定受信システムでは、送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置は、この共通の鍵データを保持する鍵保持手段を具備し、いずれのチャンネルが選局された場合でも鍵保持手段に保持された共通の鍵データを用いてデスクンランブルする。

【０００８】そのため、受信装置では、受信中のチャンネルが、別の視聴権のあるチャンネルに切り替えられた場合でも、共通情報ＥＣＭの受信を待たずに、保持しているスクランブル鍵を用いて、切り替えたチャンネルのデータをデスクランブルすることができる。

【０００９】

【発明の実施の形態】本発明の請求項１に記載の発明は、複数のチャンネルデータをスクランブルするための鍵データを生成する鍵生成手段と、鍵データを用いてチャンネルデータをスクランブルするスクランブル手段とを具備する送信装置と、複数のチャンネルの中から選択した任意のチャンネルをこの鍵データを用いてデスクランブルするデスクランブル手段を具備する受信装置とから成る限定受信システムにおいて、送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置が、この共通の鍵データを保持する鍵保持手段を備え、いずれのチャンネルを選局した場合でも鍵保持手段に保持された共通の鍵データを用いてデスクンランブルするようにしたものであり、受信装置では、受信中のチャンネルを別の視聴権のあるチャンネルに切り替える場合に、共通情報ＥＣＭの受信を待たずに、そのチャンネルのデータをデスクランブルし、視聴が可能になる。

【００１０】請求項２に記載の発明は、送信装置が、鍵データを格納する関連情報の中に共通の鍵データを含めて送信し、受信装置は、関連情報から取得した共通の鍵データを鍵保持手段で保持するようにしたものであり、送信装置は、各チャンネルデータを共通の鍵データを用いてスクランブルする場合には、その鍵データを関連情報（即ち、個別情報ＥＭＭ及び共通情報ＥＣＭ）で送信し、受信装置は、関連情報から取得した共通の鍵データを保持して各チャンネルのデスクランブルに使用する。

【００１１】請求項３に記載の発明は、送信装置が、鍵データを格納した関連情報に鍵データが共通の鍵データであるか否かを示す識別情報を含めて送信し、受信装置は、共通の鍵データを示す識別情報が含まれた関連情報から鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに関連情報から鍵データを取得する汎用鍵復号モジュールとを具備し、関連情報に共通の鍵データを示す識別情報が含まれているときは、特殊鍵復号モジュールによって取得され、鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、関連情報に共通の鍵データを示す識別情報が含まれていないときは、汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルするようにしたものであり、一台の受信装置で、請求項１の限定受信方式と従来の一般的な限定受信方式の二通りの方式に対応することができる。

【００１２】請求項４に記載の発明は、送信装置が、鍵データを格納した関連情報を送信し、受信装置は、関連情報から鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに関連情報から鍵データを取得する、実装可能な汎用鍵復号モジュールと、汎用鍵復号モジュールの実装の有無を検出する検出手段とを具備し、検出手段が、汎用鍵復号モジュールの実装を検出していないときは、特殊鍵復号モジュールによって取得され、鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、検出手段が、汎用鍵復号モジュールの実装を検出しているときは、汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルするようにしたものであり、一台の受信装置で、請求項１の限定受信方式と従来の一般的な限定受信方式の二通りの方式に対応することができる。

【００１３】請求項５に記載の発明は、受信装置の受信チャンネルが変更された場合に、特殊鍵復号モジュールは、現在受信中のチャンネルに関する情報を受けて、視聴の可否を判断するようにしたものであり、切り替えたチャンネルが視聴権を有するチャンネルであるかどうかを判断し、視聴権を有するチャンネルである場合に、共通の鍵データによるデスクランブルが開始される。

【００１４】請求項６に記載の発明は、受信装置が、受信チャンネルの変更後に受信した関連情報に基づいて、視聴の可否を確認し、視聴権が無ければデスクランブルを停止するようにしたものであり、関連情報の番組情報を照合して、視聴権が無い場合にはデスクランブルを停止することにより、限定受信のセキュリティを向上することが可能となる。

【００１５】請求項７に記載の発明は、送信装置が、関連情報に番組識別情報を含めて送信し、特殊鍵復号モジュールを持たずに、汎用鍵復号モジュールのみを具備する受信装置は、番組識別情報から視聴の可否を判断するようにしたものであり、請求項１の限定受信方式を採りながら、従来の限定受信方式の受信装置でも、限定受信処理を行うことができる。

【００１６】請求項８に記載の発明は、汎用鍵復号モジュールが、ＩＣカードで構成され、受信装置は、このＩＣカードを挿入するスロットを具備するようにしたものであり、一般的な限定受信モジュールを汎用鍵復号モジュールとして用いることが可能になる。

【００１７】請求項９に記載の発明は、受信装置が、プログラムダウンロード手段を備え、送信装置からのダウンロードにより特殊鍵復号モジュールを置き換えるようにしたものであり、特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能となる。

【００１８】請求項１０に記載の発明は、特殊鍵復号モジュールと受信装置のデスクランブラとがＰＣＭＣＩＡカードに実装され、受信装置は、このＰＣＭＣＩＡカードのスロットを具備するようにしたものであり、特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能となる。

【００１９】請求項１１に記載の発明は、送信装置が、共通の鍵データを格納した関連情報にバージョン情報を含めて送信し、受信装置は、バージョン番号が更新されるまで、鍵保持手段で保持された同一の共通の鍵データを用いてデスクランブルを続けるようにしたものであり、共通情報ＥＣＭの内容が変更されるまで関連情報を復号する必要が無くなり、受信装置の処理負荷を低減することが可能となる。

【００２０】請求項１２に記載の発明は、送信装置が、共通の鍵データを格納した関連情報に複数種類のスクランブル鍵を含めて送信し、受信装置は、複数種類のスクランブル鍵を鍵保持手段で保持し、コンテンツデータパケットの非スクランブル部の情報からどのスクランブル鍵が用いられているかを識別して、デスクランブルに用いるスクランブル鍵を選択するようにしたものであり、スクランブル鍵の更新と、共通情報の更新のタイミングとを厳密に同期を取る必要が無くなる。

【００２１】請求項１３に記載の発明は、受信装置が、番組多重情報を保持する番組多重情報保持手段を備え、番組多重情報が更新された時以外は、番組多重情報保持手段に保持された番組多重情報を基に選局するようにしたものであり、ＰＳＩの受信を待たずに選局及び関連情報の受信が可能となりチャンネル変更時のレスポンスがさらに向上する。

【００２２】以下、本発明の実施の形態について、図１～図６を用いて説明する。

【００２３】実施形態のシステムにおいて、送信装置128は、スクランブル鍵Ｋｓ、ワーク鍵Ｋｗ及び個別鍵Ｋｍｉを生成管理する鍵管理装置11と、ワーク鍵Ｋｗを格納した個別情報ＥＭＭをＫｍｉで暗号化するＫｗ暗号化部12と、スクランブル鍵Ｋｓを格納した共通情報ＥＣＭをＫｗで暗号化するＫｓ暗号化部14と、映像、データ等のコンテンツを生成するコンテンツ生成部16と、コンテンツをＭＰＥＧ２ＳＹＳＴＥＭＳ（ISO/IEC13818-1）のＴＳパケット（Transport Stream Packet）のデータフォーマットに変換するＴＳエンコーダ17と、ＭＰＥＧ２ＳＹＳＴＥＭＳのＰＳＩ（Program Specific Information）をチャンネル、番組の情報に合わせて生成する多重情報生成部125と、個別情報ＥＭＭ、共通情報ＥＣＭ、トランスポートストリーム及びＰＳＩをＭＰＥＧ２ＳＹＳＴＥＭＳ（180/IEC13818-1）の規定通りに多重化するＴＳ多重化部13と、ＴＳ多重化部13で多重化されたデータの中からコンテンツストリームのみをスクランブル鍵Ｋｓでスクランブルするスクランブラ15と、送信データを６４Ｑ変調する６４Ｑ変調部18と、変調した信号を周波数多重する周波数多重部126とを備えている。

【００２４】一方、受信装置110は、伝送路19より受信

した信号を周波数分離する周波数分離部127と、受信信号を６４ＱＡＭ復調する６４ＱＡＭ復調部111と、受信信号からＰＳＩ、映像ストリーム、共通情報ＥＣＭ、個別情報ＥＭＭ等を分離するＴＳ分離部112と、選局されたチャンネルの映像ストリームをＫｓを用いてデスクランブルするデスクランブラ114と、デスクランブルされたストリームをコンテンツストリームの形式に変換するＴＳデコーダ123と、コンテンツストリームを視聴可能なアナログ信号に変換するＡＶデコーダ124と、ＰＳＩ情報に基づいてフィルタリングすべきＰｒｏｇｒａｍ－ＩＤをＴＳ分離部112やデスクランブラ114等に伝える制御ＣＰＵ113と、Ｋｓを復号化する特殊鍵復号モジュール115と、ＩＣカードで構成される、Ｋｓを復号化する汎用鍵復号モジュール116とを備えている。

【００２５】特殊鍵復号モジュール115は、送信側が複数のチャンネルに共通のＫｓを用いる場合に、そのＫｓの復号化を行うものであり、ＥＭＭを、あらかじめ持っている個別鍵Ｋｍｉ117で復号化してＫｗを取り出すＫｗ復号化部118と、ＥＣＭをＫｗで復号化してＫｓを取り出すＫｓ復号化部119とを備えており、このＫｓ復号化部119には制御ＣＰＵ113から選局したチャンネルが伝えられる。

【００２６】また、ＩＣカードで構成される汎用鍵復号モジュール116は、送信側が複数のチャンネルに共通のＫｓを用いない場合に、そのＫｓの復号化を行うものであり、特殊鍵復号モジュール115と同様に、ＥＭＭを個別鍵Ｋｍｉ120で復号化してＫｗを取り出すＫｗ復号化部121と、ＥＣＭをＫｗで復号化してＫｓを取り出すＫｓ復号化部122とを備えている。この汎用鍵復号モジュール116は、ＩＣカードを取り替えることによって交換可能である。

【００２７】まず、このシステムでの送受信の概要に関して説明する。

【００２８】送出側では、鍵管理装置11がワーク鍵Ｋｗを生成し、これを個別情報ＥＭＭに格納した後に、Ｋｗ暗号化部12が、個別情報ＥＭＭをあらかじめ鍵管理装置11から受け取っているＫｍｉを用いて暗号化し、暗号化された個別情報としてＴＳ多重化部13に送出する。ＴＳとはＭＰＥＧ２ＳＹＳＴＥＭＳ（ISO/IEC13818-1）におけるTransport Stream Packetのことである。

【００２９】また、スクランブル鍵Ｋｓは、鍵管理装置11が生成し共通情報ＥＣＭに格納した後に、Ｋｓ暗号化部14が、共通情報ＥＣＭをあらかじめ鍵管理装置11から受け取っているＫｗを用いて暗号化し、暗号化された共通情報としてＴＳ多重化部13に送出する。

【００３０】また、映像、データ等のコンテンツは、コンテンツ生成部16よりＴＳエンコーダ17に送られ、ＭＰＥＧ２ＳＹＳＴＥＭＳ（ISO/IEC13818-1）におけるＴＳパケット（Transport Stream Packet）のデータフォーマットに変換される。ＴＳ化された映像情報等のコンテンツデータはＴＳ多重化部13に送られる。

【００３１】また、マルチプログラム構成の場合は、コンテンツデータは複数のコンテンツ生成部からそれぞれのＴＳエンコーダに送られ、ＴＳエンコーダ17はコンテンツデータをＴＳパケット化しＴＳ多重化部13に送る。

【００３２】また、多重情報生成部125では、ＭＰＥＧ２ＳＹＳＴＥＭＳのＰＳＩをチャンネル、番組の情報に合わせて生成し、ＴＳ多重化部13に送る。

【００３３】ＴＳ多重化部13に送られた個別情報ＥＭＭ、共通情報ＥＣＭ、コンテンツストリーム及びＰＳＩは、ＭＰＥＧ２ＳＹＳＴＥＭＳ（180/IEC13818-1）での規定通り多重化され、スクランブラ15に送られる。スクランブラ15では、Ｋｓ暗号化部14から渡されたスクランブル鍵Ｋｓを用いてコンテンツストリームのみをスクランブルし、スクランブルされたトランスポートストリームを６４Ｑ変調部18に送り６４ＱＡＭ変調する。さらに他に６４ＱＡＭ変調された信号とともに周波数多重部126において周波数多重を行い、伝送路19に送出する。

【００３４】一方、受信装置110では、伝送路19より受信した信号を周波数分離部127で周波数分離し、６４ＱＡＭ復調部111で復調し、復調された信号がＴＳ分離部112で分離される。

【００３５】制御ＣＰＵ113は、受信装置操作部で選局したチャンネルのＰＳＩ情報を基にフィルタリングすべきＰｒｏｇｒａｍ－ＩＤを取得してＴＳ分離部112に伝達し、それによって、ＴＳ分離部112では、該当チャンネルの復調されたトランスポートストリームを関連情報（以下、共通情報ＥＣＭ、個別情報ＥＭＭの総称とする）と、映像ストリーム等とに分離することが可能になる。また、制御ＣＰＵ113は、デスクランブルするＰｒｏｇｒａｍ－ＩＤをデスクランブラ114に設定し、選局したチャンネルをＫｓ復号化部119に設定する。

【００３６】また、受信装置110は、受信装置内回路基板に実装された特殊鍵復号モジュール115と、ＩＣカードで構成される汎用鍵復号モジュール116とを持ち、ＴＳ分離部112により分離された関連情報は、特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれかに送られ、そこで、コンテンツをデスクランブルするためのスクランブル鍵Ｋｓが取り出される。

【００３７】例えば、特殊鍵復号モジュール115を用いた場合では、ＴＳ分離部112により分離された個別情報ＥＭＭは、Ｋｗ復号部118で、あらかじめ持っている個別鍵Ｋｍｉ117を使って復号され、個別情報ＥＭＭ内に格納されたワーク鍵Ｋｗが取り出されてＫｓ復号部119に設定される。また、ＴＳ分離部112により分離された共通情報ＥＣＭは、Ｋｓ復号部119で、先に取り出されたワーク鍵Ｋｗを使って復号され、共通情相ＥＣＭ内に格納されたＫｓが取り出されてデスクランブラ114に設定される。

【００３８】ＴＳ分離部112で分離された映像などのコ

ンテンツストリームは、デスクランブラ114において、セットされたスクランブル鍵Ｋｓを使ってデスクランブルされ、ＴＳデコーダ123に送られてコンテンツストリームの形式に変換され、さらに映像はＡＶデコーダ124により視聴可能なアナログ信号に変換される。

【００３９】以上が送受信方法の概略であるが、次に共通情報ＥＣＭ及び個別情報ＥＭＭの具体内容を示しながら、より詳細な送受信方法について述べる。

【００４０】送信側の処理として、まず、鍵管理装置11は、図３に示すデータフォーマットの個別情報ＥＭＭを各受信装置毎に生成する。また、Ｋw暗号化部12は、図３に示すデータフォーマットの暗号部のみを個別鍵Ｋｍｉで暗号化し、ＴＳパケット化してＴＳ多重化部13を通して、番組の送信に先立ってあらかじめ送信する。

【００４１】個別情報ＥＭＭの各フィールドの意味は次のとおりである。非暗号部のモジュール識別フラグには特殊鍵復号モジュール115または汎用鍵復号モジュール116のどちらを用いるかを識別する情報が入る。ここでは特殊鍵復号モジュール115を示す識別情報を入れる。受信装置ＩＤには受信装置を識別するＩＤを入れる。バージョン情報には受信装置ＩＤ毎に個別情報のバージョン情報を入れる。すなわち送出側では、受信装置に個別情報を送る際に、受信装置ＩＤ毎の個別情報を更新する毎にバージョン情報の値をインクリメントして送出する。暗号化されるフィールドには、ワーク鍵と、該当する受信装置ＩＤに対して付与する個別オーソライズ情報とを入れる。

【００４２】また、鍵管理装置11は、図２に示すデータフォーマットの共通情報ＥＣＭを各チャンネル毎に生成する。Ｋｓ暗号化部14は、ワーク鍵Ｋwを使って図２に示すデータフォーマットの暗号部のみを暗号化し、ＴＳパケット化してＴＳ多重化部13を通して送信する。

【００４３】共通情報ＥＣＭの各フィールドの意味は次のとおりである。前述の個別情報ＥＭＭと同様に、非暗号化部にモジュール識別フラグとバージョン情報とを付与する。ただし、バージョン情報は、暗号部の番組識別情報などスクランブル鍵以外が更新された場合にのみ、全チャンネルの共通情報のバージョン情報が一斉に更新される。通常はバージョン情報には番号を設定し、更新毎にインクリメントして設定する。

【００４４】また、暗号部には、スクランブル鍵と番組識別情報等とを入れる。スクランブル鍵は、各チャンネル共通の鍵を２種類スクランブル鍵１、スクランブル鍵２として設定する。ある一時点で使われているスクランブル鍵がいずれであるかという情報はコンテンツストリームのＴＳパケットヘッダにおけるｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ－ｃｏｎｔｒｏｌにて設定する。例えば、スクランブル鍵Ｋｓの更新は、スクランブル鍵１と、スクランブル鍵２とを互いに交代に１分ごとに行う。

【００４５】Ｋｓ暗号化部14は、スクランブラ15に対し、スクランブル対象のコンテンツストリーム全てに共通にＫｓを設定する。また、Ｋｓ暗号化部14は、それぞれのチャンネル毎に共通のスクランブル鍵をセットした共通情報ＥＣＭを生成し送出する。

【００４６】一方、受信装置110では、関連情報を受信した場合に、ＴＳ分離部112において関連情報のモジュール識別フラグの情報を参照し、そのフラグに応じて、特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれかに、その関連情報を振り分けて送る。

【００４７】特殊鍵復号モジュール115に送られた個別情報ＥＭＭは、Ｋw復号化部118において、受信装置ＩＤが該当受信装置と一致し、さらにバージョン情報より前回受信した個別情報から更新されていると判断された場合にのみ、個別鍵Ｋｍｉ117で復号され、Ｋwと個別オーソライズ情報とが取り出されてＫｓ復号化部119に設定される。なお、受信装置ＩＤによるフィルタリングはＴＳ分離部112であらかじめ行っても良い。

【００４８】また、ＴＳ分離部112において、共通情報ＥＣＭを受信し、モジュール識別フラグに基づいて特殊鍵復号モジュール115に振り分ける場合には、まず、現在受信中の共通情報ＥＣＭが特殊鍵復号モジュール115で復号処理されていることを制御ＣＰＵ113に通知する。次に、共通情報ＥＣＭが入力したＫｓ復号化部119では、バージョン情報が前回受信した共通情報から更新されていると判断した場合にのみ、そのＥＣＭを先にセットされたワーク鍵Ｋwを用いて復号する。そして、復号したデータから個別オーソライズ情報と番組識別情報とを比較し、チャンネル視聴権がある場合にのみ、スクランブル鍵１とスクランブル鍵２とを取り出し、両方の鍵をデスクランブラ114に設定する。

【００４９】デスクランブラ114は、コンテンツストリームのＴＳパケットヘッダにおけるｔｒａｎｓｐｏｒｔ－ｓｃｒａｍｂｌｉｎｇ－ｃｏｎｔｒｏｌを参照して、スクランブル鍵１またはスクランブル鍵２のいずれを用いてデスクランブルするかをＴＳパケット毎に選択する。また、これらの鍵は、後述するチャンネル変更時の処理のためにＫｓ復号化部119で保持される。

【００５０】次に、受信装置操作部でチャンネルを変更した時の処理について説明する。

【００５１】チャンネルが変更されると、制御ＣＰＵ113は、現在使われている復号モジュールが特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれであるかを前述の通知情報から判断し、特殊鍵復号モジュール115を使用している場合には、制御ＣＰＵ113からＫｓ復号化部119に直接、変更されたチャンネル情報を通知する。

【００５２】Ｋｓ復号化部119は、通知されたチャンネルが視聴権のあるチャンネルであるかどうかを個別オーソライズ情報から判断し、視聴権がある場合には、既に

保持しているスクランブル鍵Ｋｓをデスクランブラ114に設定する。スクランブル鍵がＫｓ復号化部119に設定されていない場合には、新たな共通情報ＥＣＭを受信し、復号化してスクランブル鍵Ｋｓを取り出す。チャンネルを変更後も共通情報ＥＣＭを受信して番組識別情報を取り出し、個別オーソライズ情報と比較参照した結果、視聴権が無ければデスクランブラ114へのＫｓへの供給を停止する。

【００５３】なお、受信装置110において、チャンネル変更後に新たに共通情報から受信チャンネルの確認検証を行わない場合には、共通情報内に番組識別情報は不要である。この場合は共通情報自体も各チャンネルで共通にすることが可能である。

【００５４】また、受信装置110において、特殊鍵復号モジュール115とデスクランブラ114とをフラッシュＲＯＭに実装し、送信装置からのデータダウンロードにより特殊鍵復号モジュール115の復号方式、アルゴリズム、デスクランブル方式を置き換えるようにしても良い。

【００５５】また、特殊鍵復号モジュール115とデスクランブラ114とをＰＣＭＣＩＡカードに実装し、受信装置110にはＰＣＭＣＩＡスロットを設け、ＰＣＭＣＩＡカードを入れ替えることにより特殊鍵復号モジュール115の復号方式、アルゴリズム、デスクランブル方式を置き換えるようにしても良い。

【００５６】次に、特殊鍵復号モジュールを持たず、汎用鍵復号モジュール116のみを持つ受信装置において、特殊鍵復号モジュール用の関連情報を用いて受信する場合について述べる。これは送信側は本方式のシステムを用い、受信側はＩＣカードなどによってＣＡ方式を変更することができる機能のみ持った従来の汎用的な受信装置である場合を想定しており、本限定受信方式は、こうした受信装置においても、チャンネル変更時の高速化の効果は得られないものの、限定受信処理自体は問題なく行われることを説明する。

【００５７】この受信装置の構成図を図６に示す。図１の受信装置に比べて、特殊鍵復号モジュール115が無い点だけが相違している。

【００５８】この従来の汎用的な受信装置では、特に関連情報のモジュール識別フラグの情報を参照する仕組みは無いので、ＴＳ分離部112は、個別情報ＥＭＭに含まれる受信装置ＩＤが該当受信装置と一致し、さらに、そのバージョン情報より前回受信した個別情報から更新されていると判断した場合には、全ての個別情報ＥＭＭを汎用鍵復号モジュール116に送る。

【００５９】汎用鍵復号モジュール116では、Ｋｗ復号化部121が、あらかじめ持っている個別鍵Ｋｍｉ120を用いてＥＭＭを復号し、Ｋｗと個別オーソライズ情報とを取り出してＫｓ復号化部122に設定する。また、共通情報ＥＣＭに関しては、Ｋｓ復号化部122が、先に設定されたワーク鍵Ｋｗを用いて復号し、復号したデータから個別オーソライズ情報と番組識別情報とを比較してチャンネル視聴権がある場合にのみ、スクランブル鍵１とスクランブル鍵２とを取り出し、Ｋｓ復号化部121に保持し、また両方の鍵をデスクランブラ114に設定する。

【００６０】デスクランブラ114は、コンテンツストリームのＴＳパケットヘッダにおけるｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌを参照して、スクランブル鍵１またはスクランブル鍵２のいずれを用いてデスクランブルするかをＴＳパケット毎に選択する。

【００６１】また、受信装置操作部によりチャンネルが変更された時には、該当するチャンネルで新たな共通情報の受信を待ち、それを受信すると復号化してスクランブル鍵Ｋｓを取り出し、コンテンツストリームをデスクランブルする。すなわち、特殊鍵復号モジュール115を有する本システム用の受信装置のように、蓄積されたスクランブル鍵を用いることは、行われない。

【００６２】次に、図１の受信装置110において、汎用鍵復号モジュール116を用いて処理する場合について述べる。これは、本発明の受信装置が、従来の一般的なＣＡ方式による受信を行う場合を想定している。

【００６３】この場合、送信側は、図５に示すデータフォーマットの個別情報ＥＭＭを送信し、また、図４に示すデータフォーマットの共通情報ＥＣＭを送信する。これらの非暗号部のモジュール識別フラグには、汎用鍵復号モジュールの使用を指定する情報が入る。また、ＥＭＭの暗号化されるフィールドには、ワーク鍵と、該当する受信装置ＩＤに対応する個別ティア情報とが入り、ＥＣＭの暗号化されるデータフィールドにはスクランブラ鍵と番組ティア情報とが入る。

【００６４】受信装置は、ＩＣカードスロットを備え、汎用鍵復号モジュール116を組み込んだＩＣカードを挿入できる構成を備えている。

【００６５】受信装置が図５に示す個別情報ＥＭＭを受信した場合に、ＴＳ分離部112は、関連情報のモジュール識別フラグの情報を参照し、そこに汎用鍵復号モジュール116の利用を求す情報が付加されているために、その個別情報をＩＣカードの汎用鍵復号モジュール116に振り分けて送る。その後の処理は、特殊鍵復号モジュール115における処理と同じであり、Ｋｗ復号化部121は、Ｋｗと個別ティア情報とを取り出してＫｓ復号化部122に設定する。

【００６６】また、ＴＳ分離部112が図４に示す共通情報ＥＣＭを受信した場合には、モジュール識別フラグに基づいて汎用鍵復号モジュール116に振り分ける前に、現在受信中の共通情報ＥＣＭが汎用鍵復号モジュール116で復号処理されていることを制御ＣＰＵ113に通知する。また、共通情報ＥＣＭが入力したＫｓ復号化部122は、特殊鍵復号モジュール115での処理と同様に、バージョン情報が前回受信した共通情報から更新されている

場合に、そのＥＣＭをワーク鍵Ｋｗで復号し、復号したデータから個別ティア情報と番組ティア情報とを比較し、チャンネル視聴権がある場合にスクランブル鍵を取り出す。ただし、取り出したスクランブル鍵は、Ｋｓ復号化部121に保持せずに、デスクランブラ114に設定する。

【００６７】次に、チャンネルが変更されると、制御ＣＰＵ113は、現在使われている復号モジュールが特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれであるかを前述の通知情報から判断し、汎用鍵復号モジュール116の場合には、何も行わない。

【００６８】受信装置110は、新たな共通情報ＥＣＭの受信を待ち、受信すると、汎用鍵復号モジュール116のＫｓ復号化部122がワーク鍵で復号化した後、番組ティア情報と個別ティア情報との組み合わせによって視聴権の可否を判断し、視聴権がある場合には共通情報内のスクランブル鍵Ｋｓをスクランブラ114に設定する。

【００６９】なお、チャンネル選択時に多重情報から該当のチャンネルのコンテンツストリームを取り出すために、チャンネル選局の都度、ＰＳＩ情報を取得して取り出すが、チャンネル選局から実際にコンテンツストリームを得るまでの時間をさらに短縮するために、受信装置にＰＳＩ情報をあらかじめ蓄積し、そのＰＳＩ情報を基に該当チャンネルのコンテンツストリーム及び関連情報の分離を行うようにしても良い。

【００７０】また、本実施の形態では、受信装置は関連情報のモジュール識別フラグを参照することにより、関連情報を特殊鍵復号モジュール115に送るか汎用鍵復号モジュール116に送るかを判断しているが、例えば、汎用鍵復号モジュール115をＩＣカードに実装している場合には、受信装置のＩＣカードスロットに物理的なＩＣカード挿入検出手段を設け、ＩＣカードが挿入されている場合は、ＩＣカード中の汎用鍵復号モジュールに関連情報を送り、ＩＣカードが挿入されていない場合には、受信装置内の特殊鍵復号モジュール115に関連情報を送付することによって関連情報の振り分けを行っても同様の効果が得られる。その場合には、関連情報にモジュール識別フラグは必要ない。

【００７１】

【発明の効果】以上の説明から明らかなように、本発明の限定受信システムでは、受信装置で受信しているチャンネルを、別の視聴権のあるチャンネルに切り替えた場合に、そのチャンネルのデータを迅速にデスクランブルすることができる。

【００７２】また、一台の受信装置で、本発明の限定受信方式にも、従来の一般的な限定受信方式にも対応することができる。

【００７３】また、従来の限定受信方式の受信装置であっても、チャンネル切り替え時の高速デスクランブルの効果は得られないが、限定受信処理自体は支障なく行うことができる。

【００７４】また、プログラムダウンロード手段を設けた受信装置や、特殊鍵復号モジュールとデスクランブラとをＰＣＭＣＩＡカードに実装した受信装置では、共通の鍵データを用いる特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能である。

【００７５】また、共通の鍵データを送信する関連情報にバージョン番号を含めることにより、受信装置では、バージョン番号が更新されるまでは関連情報の復号が不要になり、受信装置の処理負荷を低減することができる。

【００７６】また、受信装置で複数の共通の鍵データを保持し、コンテンツデータパケットの非スクランブル部の情報を基に、デスクランブルに用いるスクランブル鍵を選択する場合には、スクランブル鍵の更新と、共通情報の更新のタイミングとを厳密に同期を取る必要が無くなる。

【００７７】また、受信装置で番組多重情報を保持し、この番組多重情報を基に選局するようにしたものでは、ＰＳＩの受信を待たずに選局及び関連情報の受信が可能となりチャンネル変更時のレスポンスをさらに向上することができる。

【図面の簡単な説明】

【図１】本発明の実施形態における限定受信システムの送信装置及び受信装置の構成を示すブロック図、

【図２】本発明の実施形態の特殊鍵モジュール用共通情報のデータフォーマットを示す図、

【図３】本発明の実施形態の特殊鍵モジュール用個別情報のデータフォーマットを示す図、

【図４】本発明の実施形態の汎用鍵モジュール用共通情報のデータフォーマットを示す図、

【図５】本発明の実施形態の汎用鍵モジュール用個別情報のデータフォーマットを示す図、

【図６】本発明の実施形態の限定受信システムに適用可能な従来の汎用的な受信装置の構成を示すブロック図である。

【符号の説明】

11　鍵管理装置
12　Ｋw暗号化部
13　ＴＳ多重化部
14　Ｋｓ暗号化部
15　スクランブラ
16　コンテンツ生成部
17　ＴＳエンコーダ
18　６４Ｑ変調部
19　伝送路
110　受信装置
111　６４ＱＡＭ復調部
112　ＴＳ分離部
113　制御ＣＰＵ

114　デスクランブラ
115　特殊鍵復号モジュール
116　汎用鍵復号モジュール
117、120　個別鍵Ｋｍｉ
118、121　Ｋｗ復号化部
119、122　Ｋｓ復号化部
123　ＴＳデコーダ
124　ＡＶデコーダ
125　多重情報生成部
126　周波数多重部
127　周波数分離部
128　送信装置

【図２】

非暗号部			ワーク鍵による暗号部			
モジュール識別フラグ	バージョン情報	その他	スクランブル鍵１	スクランブル鍵２	番組識別情報	その他

【図３】

非暗号部				個別鍵による暗号部		
モジュール識別フラグ	受信装置ID	バージョン情報	その他	ワーク鍵	個別オーソライズ情報	その他

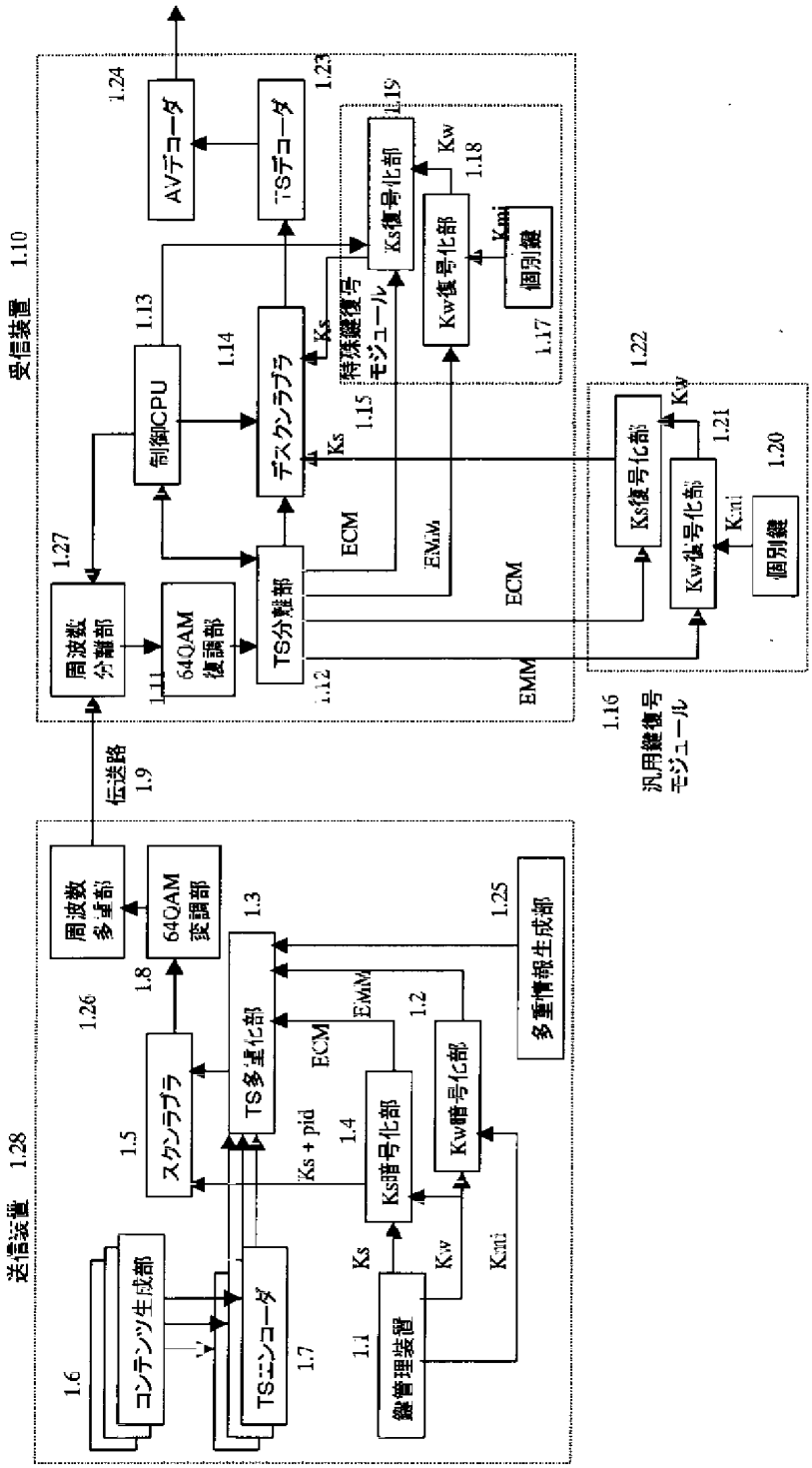
【図４】

非暗号部			ワーク鍵による暗号部			
モジュール識別フラグ	バージョン情報	その他	スクランブル鍵１	スクランブル鍵２	番組ティア情報	その他

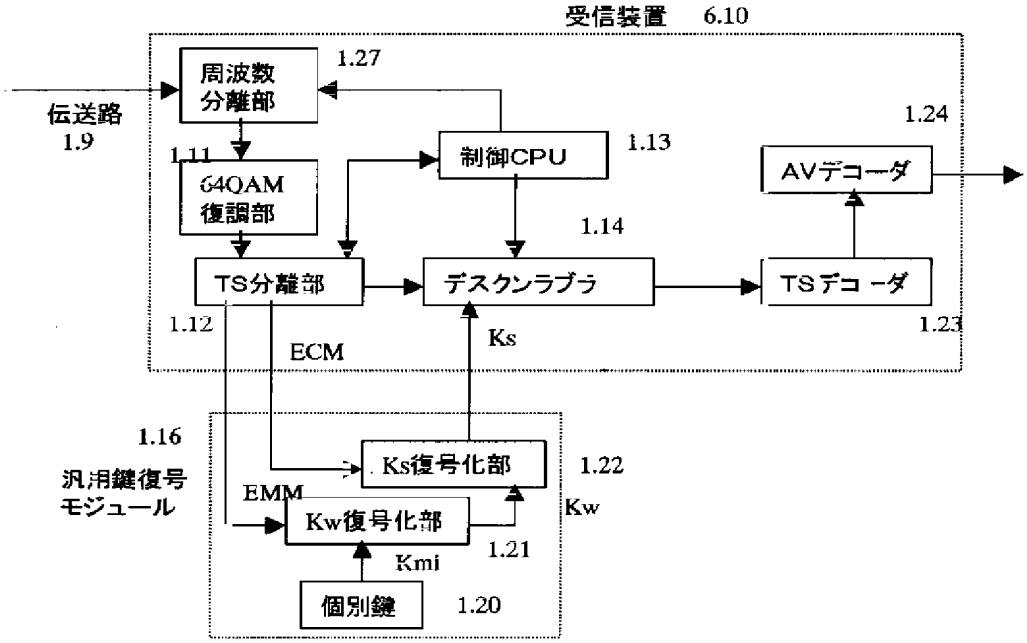
【図５】

非暗号部				個別鍵による暗号部		
モジュール識別フラグ	受信装置ID	バージョン情報	その他	ワーク鍵	個別ティア情報	その他

【図1】


送信装置 1.28
受信装置 1.10
伝送路 1.9
コンテンツ生成部 1.6
TSエンコーダ 1.7
鍵管理装置 1.1
スクランブラ 1.5
Ks暗号化部 1.4
Kw暗号化部 1.2
TS多重化部 1.3
周波数多重部 1.8
64QAM変調部 1.26
多重情報生成部 1.25
周波数分離部 1.27
64QAM復調部 1.11
TS分離部 1.12
制御CPU 1.13
デスクランブラ 1.14
特殊鍵復号モジュール 1.15
Ks復号化部 1.19
Kw復号化部 1.18
個別鍵 1.17
AVデコーダ 1.24
TSデコーダ 1.23
汎用鍵復号モジュール 1.16
Ks復号化部 1.22
Kw復号化部 1.21
個別鍵 1.20
Ks
Kw
Kmi
ECM
EMM
Ks + pid

【図６】


受信装置 6.10
周波数
分離部
1.27
伝送路
1.9
1.11
64QAM
復調部
制御CPU
1.13
1.24
AVデコーダ
1.14
TS分離部
デスクランブラ
TSデコーダ
1.12
1.23
ECM
Ks
1.16
汎用鍵復号
モジュール
Ks復号化部
1.22
EMM
Kw復号化部
Kw
1.21
Kmi
個別鍵
1.20